GRED Web Security Verification Cloud

Fully-Automated, Cloud-Based Continuous Vulnerability Assessment

(whitepaper revision 2020-NOV)

SecureBrain
A Hitachi Group Company

Overview

Across several industries, research has shown a 424% increase in security cyberattacks on business websites. This number is particularly daunting, considering how 77% of companies have reported at least one attack during the same year. The trend has forced most operations to improve website security to prevent future breaches by performing traditional vulnerability assessments.

Traditional vulnerability assessments remain effective when it comes to detecting security vulnerabilities. Moreover, this type of security measure is required for companies that use online platforms for money transactions. Vulnerability assessments are required in order to be PCI DSS compliant.

However, with that said, zero-day vulnerabilities are being discovered more frequently; thus, traditional vulnerability assessments and security solutions such as WAF are no longer sufficient on their own to address these issues, as this paper will explain.

We at SecureBrain know that the first step in finding a solution is familiarizing yourself with the problem. As websites have long become the norm, the increase in cyberattack cases is the obvious natural progression. SecureBrain has a solution called GRED Web Security Verification Cloud to help address recent vulnerability issues that were not covered by vulnerability assessments performed a while back, and GRED Web Security Verification Cloud is intended to complement and not replace existing traditional vulnerability assessments.

What Are Common Website Security Vulnerabilities?

There are several ways cybercriminals can get access to secure data within your website. Being proactive and prepared for popular methods of cyberattacks is key to preventing or minimizing the effects of an attack.

In 2017, The Open Web Application Security Project Foundation, otherwise known as the OWASP Foundation, laid out the top ten most common critical web security risks you should be wary of.

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities
- Broken Access Control
- Security Misconfiguration
- Cross-site Scripting XSS
- Insecure Deserialization
- Using Components of Known Vulnerabilities
- Insufficient Logging and Monitoring

What Are the Motives for Web Attacks?

The motive behind cyberattacks vary. Motives differ from hacker to hacker. However, for the most part, breaches are motivated by financial gain, political or social ideology, competition, or test of ability.

What Industries Are Most Vulnerable?

All companies that own a website are vulnerable to cyberattacks. However, there are industries that tend to be targeted. Due to sensitive information and data that can be easily exploited, government agencies, healthcare, finance and construction industries are amongst the highest risk.

What Are The Damaging Consequences of CyberAttacks?

At its most severe, a cyberattack can cause a financial blow to your business. Hackers, at present, are capable of executing unauthorized transfers and fraudulent monetary claims. Aside from the obvious repercussions, loss of productivity, the cost of recovery and repair, as well as legal fees, can also be a result of a cyberattack.

Moreover, your website is a reflection of your company's operation. A breach in your online presence sends a statement to your clients and potential customers that your business might not be the safest, nor is it trustworthy. As a business owner, there are very few things that are more valuable than consumer trust. Trust can make or break your brand's reputation.

Typical Solutions And Its Challenges

Developing a website for your business is both a commitment and an investment. A website that produces results is a product of mindful planning and decisiveness. Protecting the website that you build is a continuous process that takes as much commitment and investment.

Threats to web applications have existed for as long as there have been websites. Typical solutions include:

Preventative Security

Vulnerability assessments are one of the most popular forms of preventative security measures. This option reviews the weaknesses of a website, assigns a level of severity to the vulnerabilities, and suggests solutions, if ever a need arises. While effective, websites are dynamic. Constant changes in the pages render vulnerability checks useless.

Active Security

A WAF is designed to protect web applications against cross-site forgery, file inclusion, XSS, and SQL injection by filtering and monitoring HTTP traffic that is processed between a web application and the Internet. While this traditionally worked, it may not be enough for today's more advanced cyberattacks. WAFs have limited contextual information and are only able to see one raw packet at a time, making it much more challenging to provide a complete inspection perspective. In addition to that, WAFs are also not engineered for a set-and-forget approach and will require a security expert to configure, manage, and maintain it.

Response Readiness

As the name suggests, this form of security assesses a system following an attack. It includes backing-up data, doing a forensic scan, and monitoring the effects imposed by the hacker. While this response is effective for the next attack, damage has already been done.

What is Traditional Vulnerability Assessment

Traditional vulnerability assessments are a form of preventative security that reviews a website's weaknesses, evaluates its susceptibility to an attack, creates a hierarchy of the security threats, and recommends other means of protection. Traditional vulnerability assessments would require the primary involvement of a cybersecurity specialist from the vendor-side, thus making it expensive because it is human-driven.

Traditional vulnerability assessments can come in different forms depending on the company you hire to conduct them. Nevertheless, this security measure is a lengthy process. It can take up to a few months from the initial interview to the release of the report. For the most part, a vulnerability assessment involves the following steps:

Interview and Inspection

At this stage of the assessment, an IT specialist would be interviewing the website developers to have a clearer idea of how the website was built. This point is where contracts are signed, and the specialist walks the client through the impending assessment process. Between the interviews, inspections, and contract signing, this step can take a month to accomplish.

Scanning

After finalizing the logistics of the transaction, the IT specialist would then proceed to scanning the system. This process entails the use of a third-party scanning program that would sift through the website and identify the vulnerabilities that need to be addressed. Depending on the size of the system, this step could take a week.

Analysis and Risk Assessment

With the list of vulnerabilities in tow, it is time to evaluate the risks and identify the root cause of the website's security issues. These issues are ranked based on urgency, and recommendations are deliberated in order to mitigate the effects of a possible attack.

Reporting

The final step of vulnerability assessment involves creating a detailed report that would be sent to the client. Again, depending on the size of the system and the number of existing issues, the report could take two weeks to create.

Why Traditional Vulnerability Assessment Is No Longer Enough

Truth be told, existing website security options like vulnerability assessments have some efficacy level when it comes to preventing and minimizing the effects of an attack. In fact, it is an integral part of a secure website.

Nevertheless, while traditional vulnerability assessments are effective, the process, from interview to reporting, takes a long time. A good assessment takes at least a few months to accomplish. In that span of time, your website is vulnerable to attacks. After all, these assessments only detect issues that are found at the time the service is performed. While thorough, it isn't an accurate and up-to-date snapshot of your website's health.

Moreover, this type of security measure is quite an investment. Because of the cost, it can only be done a few times a year. In between periods of assessments, new zero-day vulnerabilities can be identified, and an attack can occur. With that said, while important, it isn't enough measure to protect your website.

Pros and Cons of Traditional Vulnerability Assessment

Your website is an investment in your company's image. Protecting it is imperative. Weighing the pros and cons of the security measures available should be one of your priorities.

At present, various security measures go beyond the protection traditional vulnerability assessments have to offer. Nevertheless, this option can still hold value for your operation.

Pros of Traditional Vulnerability Assessment

Detailed Report

Vulnerability assessments are thorough. This security option would give a client a clear picture of the level of protection their system has and provide means to further that stronghold.

Proactive Measure Before an Attack

As they say, prevention is better than cure. That statement rings through even for a website. Vulnerability Assessment provides a means of protection even before an attack.

Cons of Traditional Vulnerability Assessment

Lengthy Process

As mentioned earlier, the entire vulnerability assessment process can take more than a month to accomplish and cannot be feasibly performed frequently. During these time gaps in-between assessments, your website is vulnerable to attacks. Moreover, because it takes so long, information from the assessment might not be relevant or encompassing at the end of the process.

Expensive

Vulnerability assessments are notorious for being expensive. This security measure employs not only the expertise of an IT professional but also a third-party program to conduct tests regularly.

How to Secure Your Website Today

An attack on your website can have a severe effect on your business. According to a study conducted by A James Clark School of Engineering, hackers attack every 39 seconds. Each year, these cybercrimes get more sophisticated.

Implementing different levels of security can be the key to protect your website truly. Learn about the top security options available for you this 2020:

HTTPS Protocols

Ensuring that your website uses HTTPS protocols is excellent for several reasons. For one, search engines identify pages that do not use HTTPS protocols and immediately warn visitors before accessing the site. The most crucial benefit of using HTTPS protocols is that it is more difficult for someone to eavesdrop into the website traffic to steal sensitive data.

Software Updates

Websites use a slew of software tools to provide the best user experience. Updating the system to the latest version is an excellent way to safeguard your website. Updates tackle bugs, eliminate glitches, and install security patches.

Password Management

Passwords are the easiest way to secure your website. However, they also pose the highest security risks. On average, hackers can crack a fourth of website passwords in under three seconds. Often a strong password isn't enough. Choosing to change your login credentials frequently can provide a better stronghold against hackers.

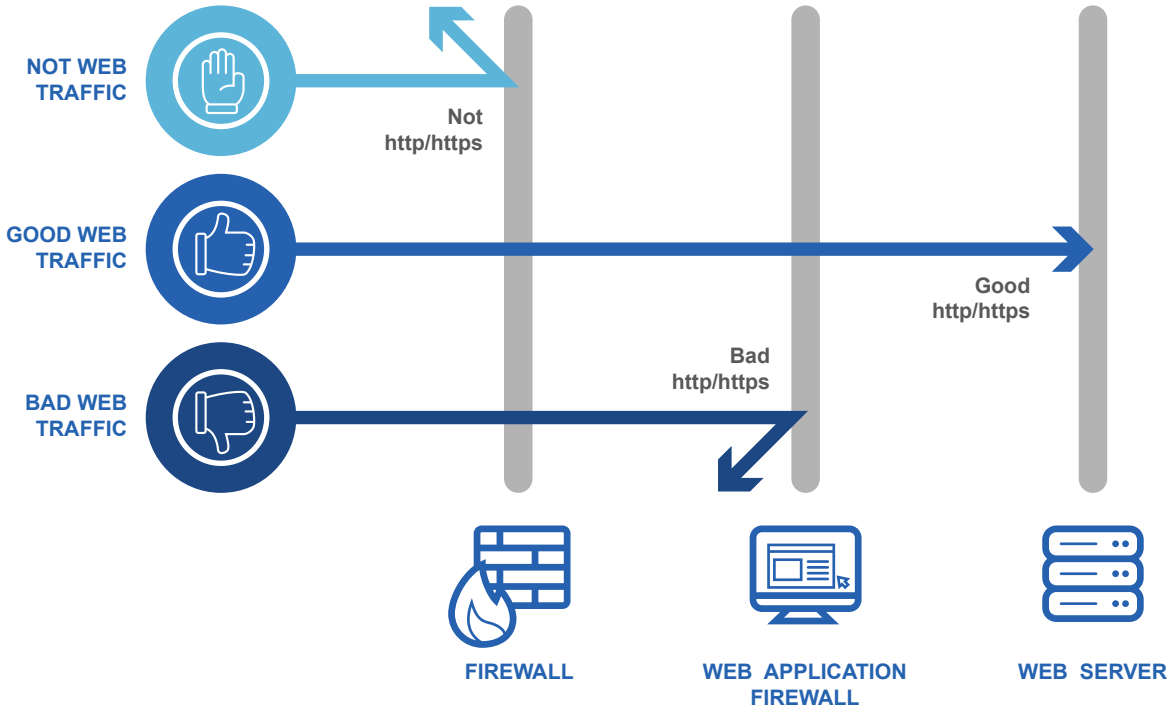
Website Backups

Despite your best security efforts, there is still a chance a hacker would be able to breach your website. Having a back-up of your system allows you to restore your website's clean version following an attack with minimal downtime.

Web Application Firewall

Otherwise known as WAF, it is a security measure that protects a website by filtering, monitoring, and subsequently blocking malicious HTTP traffic between the web application and the internet.

If done correctly, WAF can be incredibly effective in protecting your website. However, this form of website security measure requires the user to write specific rules and actions concerned with filtering, monitoring, and blocking. It isn't exactly a set-it-and-forget-it system. In fact, it involves the help of the website owner, the website developer, and a third-part WAF integrator.



Website Security Framework

Aside from the options above, an effective way to safeguard your website is by creating a website security framework that works for your operations. At its core, a website security framework is a multi-level series of security measures that aim to safeguard your system at every step of an attack. A framework typically includes five functions: identify, protect, detect, respond, and recover.

Identify

The first step in your website security framework involves identifying and cataloging the assets that need protection. Having a clear idea of the items to safeguard would make it easier for you to develop your security measures accordingly.

Protect

As discussed earlier, having traditional preventative security measures in place is essential in covering all your bases. It acts as a protective shield that makes it difficult for attacks to breach your system.

Detect

While WAF can be an effective layer of defense if properly configured, continuous monitoring is still needed to ensure that your website is clear from threats in real-time. Using security scanners that check DNS records, SSL certificates, user access, and file integrity can help in this process.

Respond

Attacks happen even to websites with impressive security infrastructure. Nevertheless, a response plan is key to mitigating the effects of an attack. This plan should include the assigned person to resolve the issue, a report of the attack, and the series of steps that need to be done to contain the situation.

Recover

A detailed account of the hacking event is the main component of the recovery stage. Reviewing the details is key to developing a security structure that can withstand the most recent attack. In this stage, it is important to discuss not only your current security measures but to open the conversation to new options that might be available to you.

Your Website is Safe with GRED Web Security Verification Cloud

In today's day and age, advancements in technology can be a blessing and a curse, especially for companies who manage their websites. Malicious attacks have become sophisticated over the last few years. Today's breaches can incur serious effects in a company's operation.

Thankfully, likewise, security measures that safeguard websites against hackers have improved with the times. At present, you can choose from several options. **GRED Web Security Verification Cloud** is amongst the best complements to traditional vulnerability assessments and not intended to be a replacement.

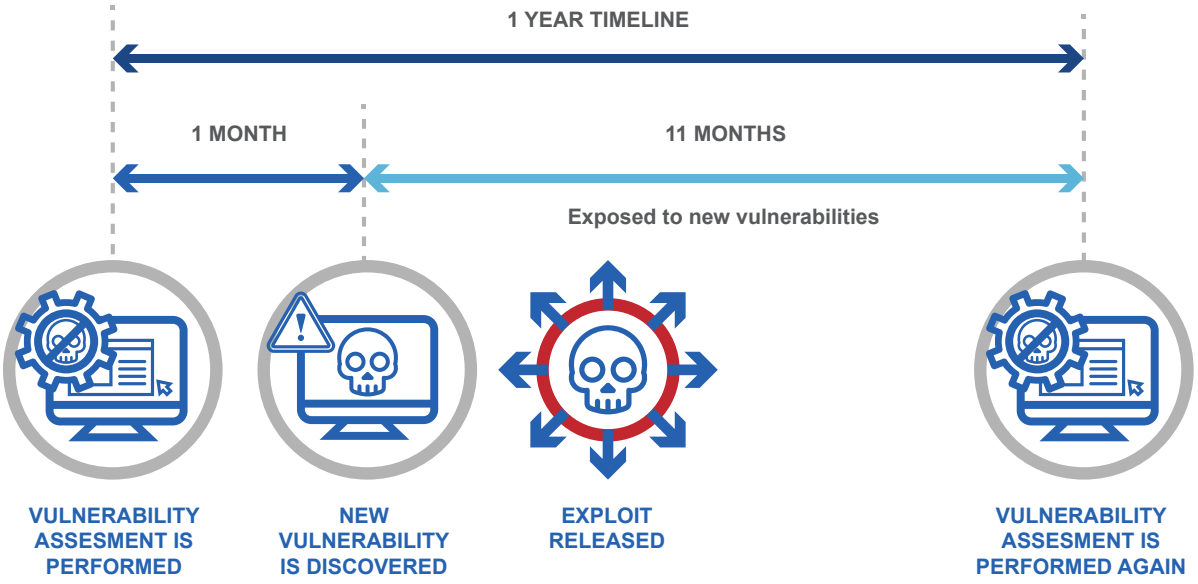
GRED Web Security Verification Cloud is a service that provides a web application a continuous form of security. It regularly checks the vulnerabilities of a website without the constant need for human supervision. It is cost-effective, easy to understand, and requires no software installation.

GRED Web Security Verification Cloud: Features and Benefits

The beauty of **GRED Web Security Verification Cloud** lies in its simplicity and ease of use. This SaaS program provides an automatic means to protect your website from various critical attacks by conducting daily Vulnerability Verifications and transcribing it in a concise and easy-to-understand report.

Unlike most vulnerability assessments, **GRED Web Security Verification Cloud** has a short lead time. Instead of two months, this program only requires your website URL. It supports most dynamic websites, requires no installation, and is a cost-effective option because of its automated process.

Why Your Organization Needs GRED Web Security Verification Cloud



GRED Web Security Verification Cloud goes hand in hand with the level of security that traditional vulnerability assessments offer.

While invaluable, traditional vulnerability assessments are expensive and can be feasibly performed once a year for most companies. This type of security measure is able to identify vulnerabilities that are present when the assessment is conducted. This means opting for a vulnerability assessment as your company's only line of defense leaves your network exposed to various cyberattacks for 11 months.

GRED Web Portal

While thorough, vulnerability assessment reports can be daunting. They are full of jargon that is intimidating for the uninitiated.

GRED Web Security Verification Cloud's web portal is as easy to understand as it is to use. The portal is intuitive and visual. It assigns colors on various risks depending on the severity of the vulnerability. The reports from the portal are archived and are downloadable in PDF format.

How GRED Web Security Verification Cloud Works

The beauty of **GRED Web Security Verification Cloud** lies in its simplicity and ease of use. This SaaS program provides an automatic means to protect your website from various critical attacks by conducting daily Vulnerability Verifications and transcribing it in a concise and easy-to-understand report.

Unlike most vulnerability assessments, **GRED Web Security Verification Cloud** has a short lead time. Instead of two months, this program only requires your website URL. It supports most dynamic websites, requires no installation, and is a cost-effective option because of its automated process.

Step 1 Onboarding

Signing up for **GRED Web Security Verification Cloud** is simple. All that the program requires is registering your website on the **GRED Web Security Verification Cloud** platform.

Step 2 Daily Website Scanning

Once the website has been registered, the program would automatically scan the website for vulnerabilities. The tool scans the site daily to ensure that the web application is protected at all times and all risks are addressed promptly.

Step 3 Email Alert

If **GRED Web Security Verification Cloud** detects a threat on your website, it will send an email alert to the website owner or system administrator detailing the vulnerability identified.

Step 4 Web Portal Report

In conjunction with the email, the web portal provides the necessary updates on the identified risk. The portal also logs possible solutions to the detected vulnerability.

Step 5 Vulnerability Mitigation

With all the threat details in tow as well as recommendations for mitigation, **GRED Web Security Verification Cloud** allows systems administrators to act promptly on detected threats. This protects and minimizes the effects of an attack on the website.

GRED Web Security Verification Cloud: A Cut Above the Rest

GRED Web Security Verification Cloud provides unmatched daily protection for web applications without the need for supervision and installation. Nevertheless, there are several companies that try to provide the same service.

GRED Web Security Verification Cloud is a cut above the rest for several reasons. Many platforms require some form of software download in order to utilize their service. **GRED Web Security Verification Cloud** is completely cloud-based. This means that opting for this security product is cost-efficient and flexible.

Moreover, onboarding with the **GRED Web Security Verification Cloud** is simple and easy. It doesn't require any interviews or face-to-face touchpoints. The process only requires the registration of your URL onto the **GRED Web Security Verification Cloud** website.

GRED Web Security Verification Cloud Partners

GRED Web Security Verification Cloud is the brainchild of SecureBrain - a leader in software services recognized worldwide. With over a decade of experience, SecureBrain has been in partnership with international companies, including Zenlogic, NetForest, Sakura Internet, NTT Data, and Marketing Bank.

Global Opportunity

Depending on your operation's size, **GRED Web Security Verification Cloud** is available in Partner or Reseller bundle options. SecureBrain also offers competitive pricing for OEM or MSSP partnerships.

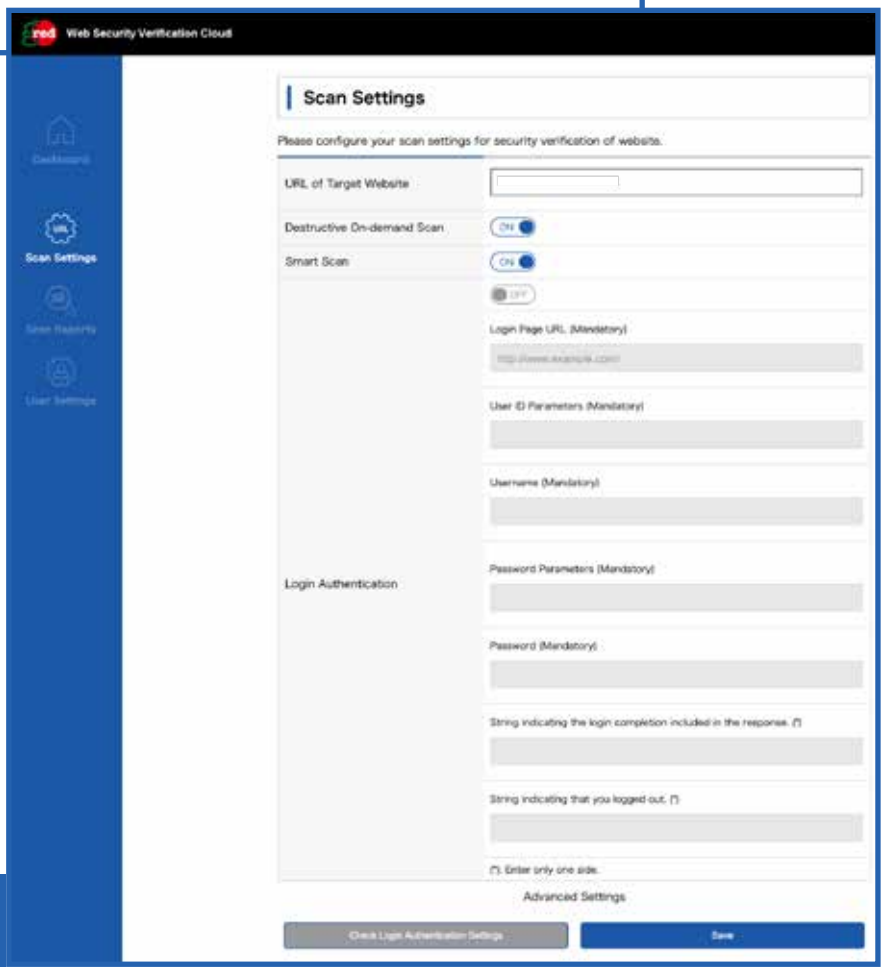
Conclusion

At the end of the day, securing your website is an investment in the growth of your business. **GRED Web Security Verification Cloud** is a security measure meant to complement the traditional safeguards you already have in place. It fills the gap between vulnerability assessments and ensures that you know where your website stands 24/7.

GRED Web Security Verification Cloud is your peace of mind.

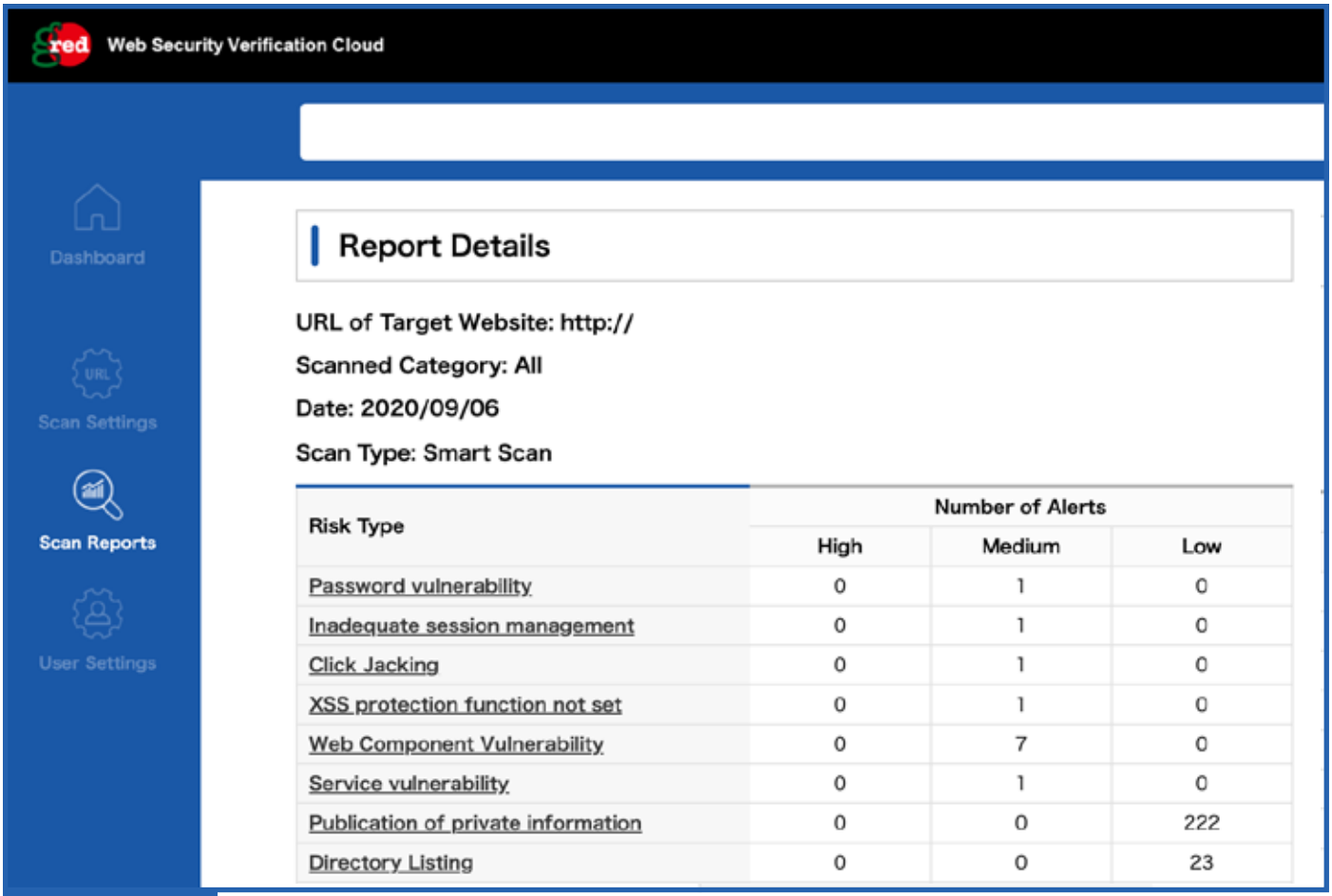
Appendix:
Screenshots of Web Portal

Dashboard



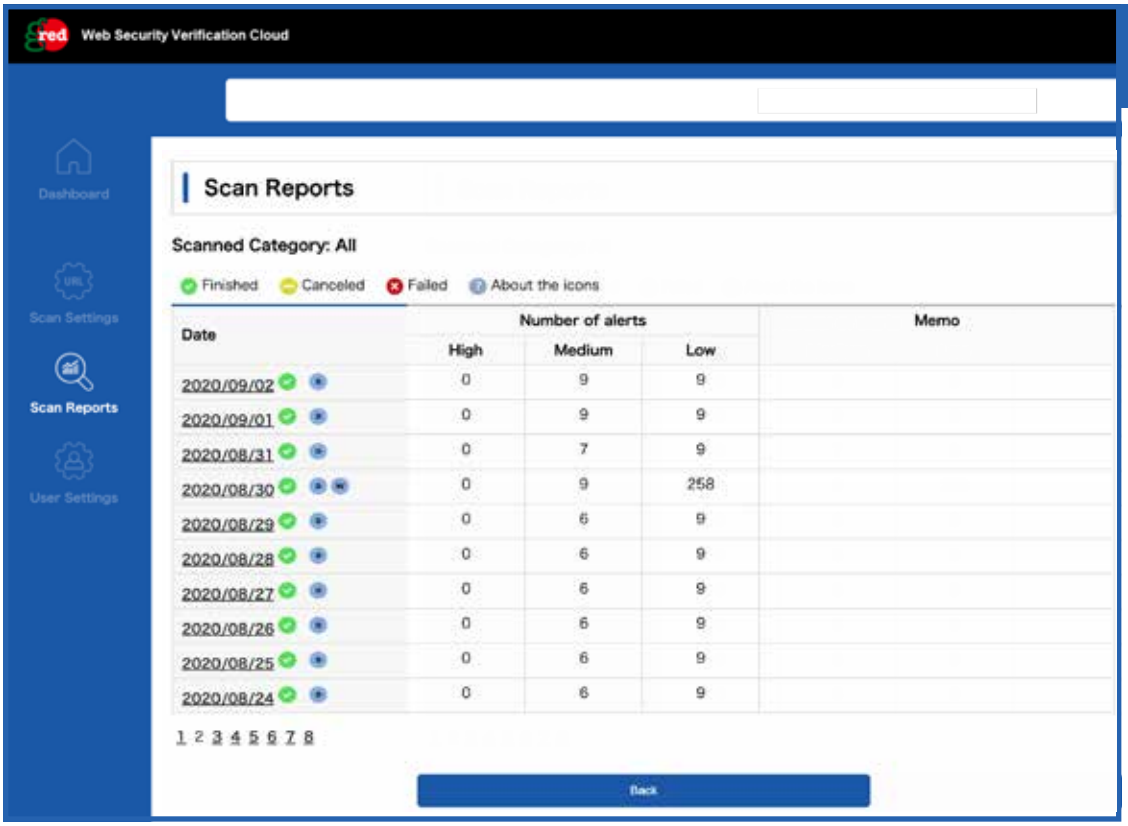
Scan Settings

SecureBrain
A Hitachi Group Company

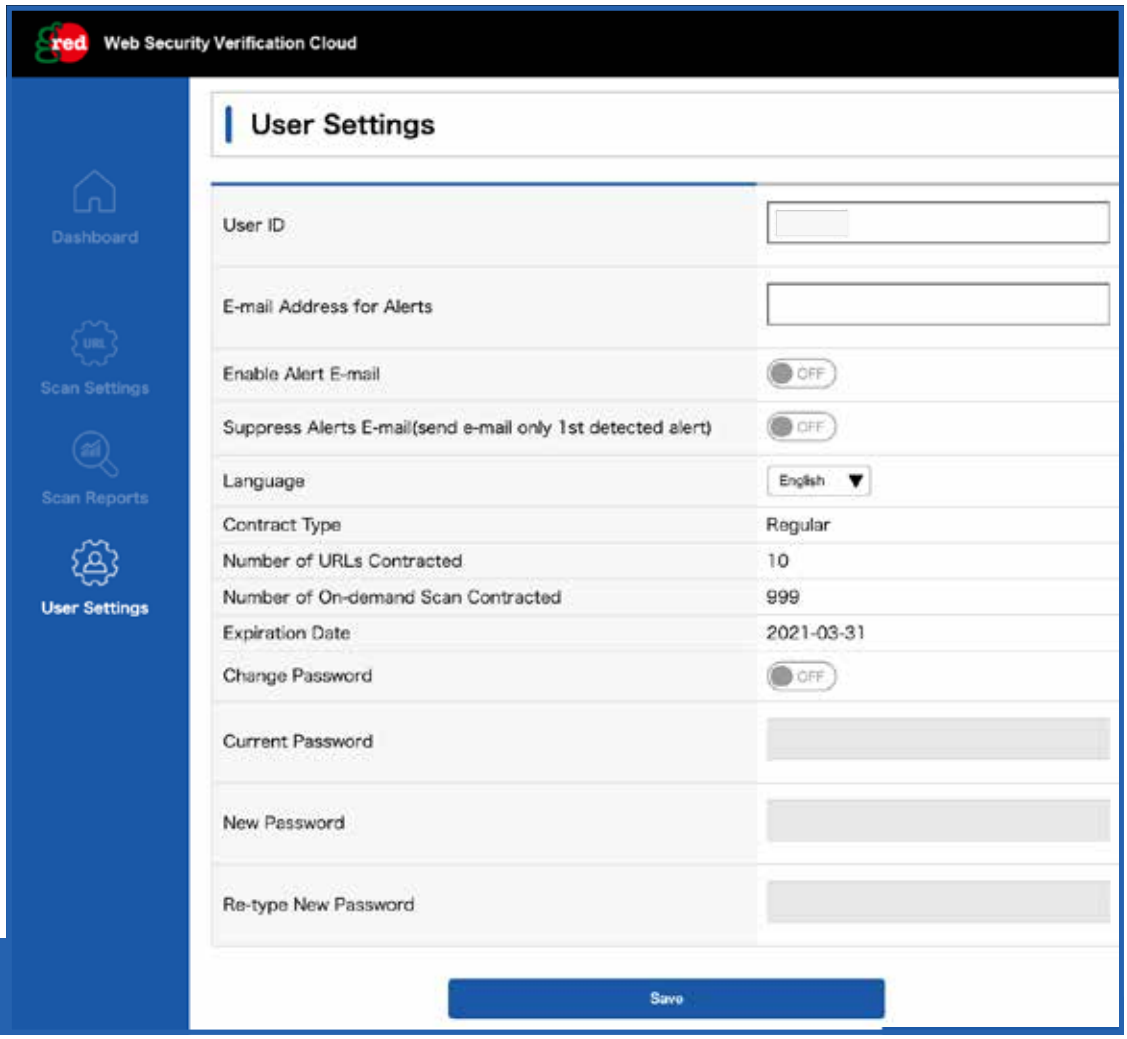


Reports List

Result Details



Scheduled Scans



User Settings

GRED Web Security Verification Cloud by SecureBrain

With almost two decades of experience, SecureBrain is considered as Japan's leading security software provider. Based in Tokyo, our company aims to provide a wide array of security options for every type of business within and outside of Japan.

SecureBrain runs its own research center in order to ensure that we are providing the leading technologies in website malware detection and protection. Our team of researchers is dedicated to identifying new online website security risks and developing solutions to current and future threats.

We have secured the business of several multinational companies as well as government contracts that are specifically geared towards cybercrime and security.

SecureBrain
A Hitachi Group Company

https://www.securebrain.co.jp/eng